Wired vs. Wireless: Examining M2M Technologies for Communication Networks in Utility Markets

By: FreeWave Technologies, Inc.

Many operators in the utility industry are looking for new ways to maximize their investment in machine-to-machine (M2M) communication networks while ensuring reliable, secure data transmission. There are a variety of communications solutions, the two most common being broadband wireless technology and high-speed wired options, such as copper and fiber-optic cable. While both have a place in the utility spaces and industrial M2M applications such as distribution automation in the smart grid, we are beginning to see an increase in the use of broadband wireless M2M technology.

FreeWave®

Wired vs. Wireless: Examining M2M Technologies for Communication Networks in Utility Markets

There are many factors contributing to the increased adoption of wireless M2M communications including cost savings, flexibility and power consumption. When looking at the big picture, a utility operator will discover that each technology has its own advantages and disadvantages. Many feel the most reliable option for a M2M communication network is the traditional wired approach, but advancements in wireless M2M networking capabilities and the proliferation of the industrial Internet of Things (IoT) have made some wired technology advantages negligible. On the other hand, with so many different types of wireless M2M technologies available today, the decision making process becomes even more complex. Expansive M2M communication networks are not one-size-fits-all, and it is critical for utility operators to understand the type of technology they need in order to have the most effective networking capabilities for their individual system. Additionally, they need to consider the economic factors when searching for the best system that their budget allows.

Applying Wireless M2M Networking Platforms to the Utility Industry

Wireless M2M communication technology can vastly improve data transmission for applications in many industries. For instance, when looking at utilities, wireless M2M networking platforms of today enable the improvement of distribution automation for the smart grid. One example is recloser control. Traditionally, this action is handled manually. By operating resclosers, electricity can be re-routed over the grid in order to bypass problem areas. By applying this industrial automation practice, both time and costs are saved, leading to optimized grid operations. This is just one example of how automating distribution automation can improve the overall performance of the smart grid.

Industrial M2M networking platforms, in particular, offer proven, reliable data transmission and advantages where:

- Remote monitoring of service delivery is required
- Maintenance crews need Wi-Fi capabilities
- Communication security is a priority
- AMI and AMR efficiency is needed
- Companies want new networks without re-trenching costs

In other words, wireless M2M networking offers utility operators a viable solution for meeting their distribution automation requirements, while also ensuring maximum efficiency and network security protocols. As the industry continues its fast-paced growth, the need to identify ways to lower infrastructure costs, improve time-to-market and increase performance with reliable, easily installed networks are no longer a wish, but, a requirement.

As the smart gird market in particular continues to make strides in the power industry, utility operators are looking for economical ways to manage their systems. To do this most efficiently, companies are turning increasingly toward wireless M2M networking technologies.

Wired versus Wireless Solutions

The families of wireless M2M networking platforms that are proven to be reliable in the harshest of environments are commonly deployed daily in mission-critical industrial applications. These platforms may offer the most effective, secure and efficient solution, when compared to other options. For example, when compared with fiber, wireless M2M systems are relatively easy to install. In the event that a buried cable is damaged to the extent that it requires repair or replacement, the costs can be very high. Many wireless M2M technologies are relatively maintenance-free, and, if maintenance does become necessary, they can be easily maintained. Once installed, industry leading wireless M2M communication devices rarely need any type of service. If, for some reason, maintenance is required, the best systems provide information regarding a pending maintenance concern and the location or type of maintenance required can easily be detected remotely. So, operators only send someone out for service if/when they need it, thereby saving time and money. If engineered and installed correctly, wireless M2M platforms will last maintenance-free for years. At least one of the wireless M2M communications manufacturers provides backwards-compatible solutions, which also saves on maintenance concerns, as well as stocking and replacement costs.

Wireless M2M Communication Systems and Options – Pros and Cons

If an operator decides that wireless is the best option for their M2M network, they have many factors to consider. The usability and ease of installation that come along with wireless brings many different options to employ communications needs. The major ones include:

Wireless Networking Platforms

The use of proprietary and standards-based wireless M2M networking systems are quite easy to install and require minimal labor; they don't require any trenching, and once set up, the networks are relatively maintenance-free. In addition, users can obtain real-time data fast. Users can be operational quickly and don't have to wait until some sort of network typology is complete. Once remote wireless M2M networks are installed, operators can monitor these nodes right away. Additionally, many of the M2M platforms available today offer multiple frequency options, such as 900 MHz, 2.4 GHz and 5 GHz unlicensed spectrums, 3G cellular, Ethernet and mesh networking. These platforms can meet any communication need in the field, remote or local.

Cell Phone/Satellite

Most cellular and satellite M2M technologies are public communication systems and, therefore, these communication infrastructures are widely dispersed to cover large areas. Carrier-based systems, such as these,

include monthly fees that add to the overall cost of ownership, potentially making it costly over time. Notoriously, cellular-based M2M systems do not have a history for being backwards compatible. Therefore replacing old technology with new solutions can be very costly. Sometimes these systems can reach extreme or remote locations where it is not feasible to lay fiber or even deploy a full wireless M2M communication network. This especially is true in the case of satellite systems. One final consideration for cellular and satellite technology is that utilities aren't able to own the network, but rather pay to use the existing network.

Hybrid Communications as Yet another Option

None of the systems described above solve all problems in all situations. Hybrid networks – a blend of different technologies –often are important to consider. Hybrid M2M networks also might include a mix of fiber, wireless, satellite or cellular technologies. A hybrid M2M networks system can be a more cost-effective and effective solution for remote networks through lower hardware unit costs, fewer points requiring monthly fee-based satellite or cellular connections, and lower power-consuming technologies.

Another Consideration for Wireless vs. Wired: The Copper Wire Theft Factor

A more recent factor in the surge of wireless M2M technology is the dramatic increase in copper theft across the U.S. The struggling economy coupled with the dramatic increase in the price of copper over the past several years, are key factors in this criminal activity. In fact, it has created such a major economic impact that in 2008, a Department of Energy report predicted copper theft costs about $1 billion per year. In March 2011, the cost of copper was nearly $5 per pound. Looking back 10 years, in March 2001, the going rate was under $1 per pound. This increase was sparked by a demand in developing nations like China and India (http://www.fbi.gov/news/stories/2008/december/copper-theft-intel-report-unclass). In alignment with this dramatic increase, copper wire theft has become a very lucrative for thieves not only in the U.S., but around the world. They are paid cash by recyclers who often provide copper to commercial scrap dealers (http://www.fbi.gov/news/stories/2008/december/copper-theft-intel-report-unclass). Without any physical proof that the copper has been stolen, these criminals easily remain under the radar. Despite the huge economic impact, there are no signs of it slowing down. With that in mind, it is critical for utility operators to take the initiative and protect their critical infrastructure.

Copper thieves often are targeting power lines, heating and cooling pipes, and grounding wires – all of which are necessary components of the modern world. According to open-source reporting, in March 2008, approximately 4,000 residents in Polk County, Fla., lost power after copper wire was stripped from an active transformer at a Tampa Electric Company (TECO) facility. The blackout cost close to $500,000 (http://www.fbi.gov/news/stories/2008/december/copper-theft-intel-report-unclass). Examples like this have operators looking for ways to prevent thefts and many are finding that using wireless technologies make them a less likely target.

Additionally, legislation across the country is working to hinder stealing of the precious metal and lobbyist groups have formed, such as the Coalition Against Copper Theft (www.coppercoalition.com) based in Washington, D.C. The Copper Coalition has continued to grow since its founding in 2008. In addition to the monetary expense of copper theft, the Copper Coalition also points out the human cost of copper wire theft, as they have identified a direct correlation with illegal drug use.

Thieves often have easy access to copper because utility sites are often remotely located. Without a security system in place, they can easily access the metal in broad daylight, stripping the infrastructure of its critical elements. Today, replacing or choosing wireless M2M communications technology as opposed to copper wire solutions is one way to fight copper theft. In the smart grid industry, most thieves are crafty enough to avoid stealing the copper wires from high-voltage electric distribution or transport lines; they instead are going for the communication networks that are copper-based. When you look at the smart grid, the consequences of disrupting critical data transmission to the grid can have expensive consequences, like the power facility in Florida. Without proper data transmission, everything from power generation to distribution can be disabled. By using wireless for communication, operators can prevent copper theft. While historically, copper communication lines were considered more secure, we are starting to see a shift in this thinking, especially in utility industries, as a direct result of copper wire theft. However, operators must understand wireless comes with its own set of security concerns. It is critical to look for a system that can handle potential threats.

Security for Wired vs. Wireless

Unlike traditional wire-lined data communication, wireless M2M networks use a multitude of methods in order to help create the strongest network possible. This provides wireless with some unique advantages, as communication endpoints don't need to be tied down to a fixed location and dependent upon a physical cable. Traditionally, wired networks were considered the most secure option for utility companies. However, wireless security capabilities have grown so much in the past five years, which these concerns are no longer so widespread. While a wired connection requires physical access to the cable, wireless M2M connections are now protected by advanced encryption methods used across industries in many applications, including mission-critical needs in the government and defense industry.

Conclusion

High costs, difficult installations, copper theft and more are driving operators to consider alternatives to wired communication solutions. In many industries around the world, including the military, wireless M2M networking platforms are considered a stronger alternative. These technologies provide long-range, reliable and affordable solutions. A wireless M2M system can potentially save a company millions of dollars in installation and maintenance fees.

However, operators need to be aware that not all M2M networking solutions are created equal. Leading industrial M2M platforms offer flexibility to perform in almost any situation. By leveraging tried and true data encryption techniques they also can offer enhanced security, easing the minds of those who trust wired for its reputation as the most secure method for data transmission. The increase of copper theft also supports the case for wireless over wired and offers a reason for operators to think twice about choosing copper wiring. Any manufacturer who has a solid product offering is likely willing to provide operators with test equipment to prove the technology before they buy it. It is easy to use, quick to install, reliable and low risk. When ROI is a key in determining the best communications solution, the benefits of wireless M2M networking solutions should be part of every decision process.

FreeWave Technologies, Inc.

5395 Pearl Parkway, Suite 100, Boulder, CO 80301 TF 866.923.6168 T 303.381.9200
For more information, visit www.freewave.com